PATENT **MS150832.02/MSFTP150US**

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence (along with any paper referred to as being attached or enclosed) is being submitted *via* the USPTO EFS Filing System on the date shown below to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Date: February 6, 2007 /Casey L. Martin/
Casey L. Martin

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

Appellant: Michael Ginsberg

Serial No: 09/671,388

Filing Date: September 27, 2000

Examiner: Syed Zia

Art Unit: 2131

Title: TRUST LEVEL BASED PLATFORM ACCESS REGULATION APPLICATION

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

Appellant's representative submits this brief in connection with an appeal of the above-identified patent application. If any additional fees are due and/or are not covered by the credit card, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1063 [MSFTP150US].

I. Real Party in Interest (37 C.F.R. §41.37(c)(1)(i))

The real party in interest in the present appeal is Microsoft Corporation, the assignee of the present application.

II. Related Appeals and Interferences (37 C.F.R. §41.37(c)(1)(ii))

Appellants, appellants' legal representative, and/or the assignee of the present application are not aware of any appeals or interferences which will directly affect, or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims (37 C.F.R. §41.37(c)(1)(iii))

Claims 1-5 and 7-20 are pending in the application. Claim 6 has been cancelled. The rejection of claims 1-5 and 7-20 is being appealed.

IV. Status of Amendments (37 C.F.R. §41.37(c)(1)(iv))

Claim amendments had not been made after the Final Office Action.

V. Summary of Claimed Subject Matter (37 C.F.R. §41.37(c)(1)(v))

A. Independent Claim 1

Independent claim 1 and its corresponding dependent claims relate to a system that regulates access to a distributed computing platform. A component is provided that analyzes an application that requests access to the distributed computing platform. (*See e.g.* Fig. 1, element 10; Application at p. 4, lines 16-21). The component determines a level of access to the distributed computing platform and applies a trust level to the application corresponding to the determined level of access. (*See e.g.* Fig. 1, element 16; Application at p. 4, lines 21-28). Another component compares the applied trust level of the application with a trust level of a module called by the application and regulates access of the application to the distributed computing platform based at least in part upon the comparison. (*See e.g.* Fig. 1, element 18; Application at p. 4, lines 23-28).

B. Independent Claim 10

Independent claim 10 and its corresponding dependent claim relates to a system for regulating access to a distributed computing platform. Means are provided for determining a trust level for an application, the application requesting access to the distributed computing platform. (*See e.g.* Fig. 1, element 16; Application at p. 4, lines 20-22). Means are also provided for applying the trust level to the application to regulate access to the distributed computing platform. (*See e.g.* Fig. 1, element 18; Application at p. 4, lines 27-28). Means are additionally provided for regulating access of the application to the distributed computing platform by analyzing a trust level of a module called by the application. (*See e.g.* Fig. 1, element 16; Application at p. 4, lines 24-27).

C. Independent Claim 12

Independent claim 12 and its corresponding dependent claims relate to a method for regulating access to a distributed computing platform. A trust level for a first module called by an application is determined, where the application is requesting access to the distributed computing platform. (*See e.g.* Fig. 6, element 112; Application at p. 8, line 30 through page 9, line 4). Access of the application to the distributed computing platform is regulated based at least in part upon the determined level of trust for the first module. (*See e.g.* Fig. 6, element 114; Application at p. 9, lines 4-10).

VI. Grounds of Rejection to be Reviewed (37 C.F.R. §41.37(c)(1)(vi))

A. Whether claims 1-5 and 7-20 are anticipated under 35 U.S.C. §102(e) by Gupta (US 6,990,492).

VII. Argument (37 C.F.R. §41.37(c)(1)(vii))

A. Rejection of Claims 1-5 and 7-20 Under 35 U.S.C. §102(e)

Claims 1-5 and 7-20 stand rejected under 35 U.S.C. §102(e) as being anticipated by Gupta (US 6,990,492). The rejection of claims 1-5 and 7-20 should be

reversed for at least the following reasons. Gupta does not disclose or suggest each and every element as recited in the subject claims.

> For a prior art reference to anticipate, 35 U.S.C. §102 requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) (*quoting Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)).

Appellant's invention as claimed relates to regulating access of an application to a distributed computer platform by way of applying and analyzing trust levels associated with the application and modules called by the application. To that end, claim 1 recites *a component that compares an applied trust level of an application with a trust level of a module* ***called by the application*** *and* ***regulates access of the application to a distributed computing platform*** *based at least in part upon the comparison.* Claim 10 recites *means for regulating access* ***of an application*** *... requesting access to a* ***distributed computing platform*** *... to the distributed computing platform by analyzing a trust level of a module called by the application*, and claim 12 recites *determining a trust level for a* ***first module called by an application****, the application requesting access to* ***the distributed computing platform****, and regulating access of the application to the distributed computing platform based at least in part upon the determined level of trust for the first module*. Gupta does not disclose or suggest the claimed aspects.

Gupta relates to a security administration system for controlling user access to data objects. For example, the cited reference includes an example where a doctor has particular access rights with respect to certain portions of a patient's file while not having access rights with respect to other portions of the patient's file. To enable such selective restriction of access to all or portions of a data object, relationships between users and data objects are defined (*e.g.,* between a doctor and a patient's data folder) and access rights are associated with each relationship. For instance, it would be desirable to provide a doctor with at least partial access to a patient's data folder. When a user requests access to a data object, a security classification for each found relationship is

determined, wherein such security classifications can be dependent upon role of the user (*e.g.,* primary care provider). Thereafter, security classification(s) assigned to the data object are determined, and the security classifications for the relationship are compared with the security classification(s) of the desirably accessed data object. A determination can then be made regarding whether the user has access (and types of access rights) based at least in part upon the comparison. (*See* col. 9, line 65 – col. 11, line 2). These access rights can be based upon a user's role, such as a type of doctor (*e.g.,* primary care provider).

As can be ascertained from even a cursory review of Gupta, the cited reference does not disclose or suggest *regulating access of* ***an application*** *to a* ***distributed computing platform*** as is recited in the subject claims. Gupta simply discloses regulating access of a user to a data object, and it is clear that the user is merely a human operator, not an *application* as claimed. Further, it must be noted and appreciated that Gupta nowhere mentions a ***distributed computing platform***, as claimed. It is an understood term of art that "distributed computing" enables a process to run a single computational task on more than one distinct computer, therefore, a distributed computing platform is a system that facilitates distributed computing. Gupta is not even tangentially related to distributed computing, and thus cannot be construed as disclosing the aforementioned claimed aspects of the invention.

Moreover, Gupta clearly fails to disclose ***a first module called by an application***, much less ***determining a trust level for the first module***. Rather, Gupta merely teaches that a user requests access to a data object, wherein the user can have predefined relationships with the object that are associated with certain access rights (*e.g.,* due to a role of the user). It remains readily apparent, however, that the user is not an application. Furthermore, even if the user could somehow be deemed to be an application, such user is not requesting access to a distributed computing platform, but rather is requesting access to a data object.

The Final Action cited lengthy passages of Gupta from col. 9, line 65 through col. 11, line 23, and col. 7, line 64 through col. 8, line 36. However, contrary to assertions in the Final Action, these passages and the remainder of the reference also fail to disclose or suggest Appellants' claimed invention. The cited sections merely disclose methods of

controlling access to information on a computer system in which the system receives an access request from a user for information about a data object. The system finds the relationship between the user and object and determines security classification for the relationship. From these citations and the aforementioned discussion, it remains abundantly clear that the entire disclosure of Gupta is drawn to a security system for merely granting or denying user access to data. The Final Action further contended that "the system of Gupta teaches controlling access, and provides an access regulation system that can analyze and interact with a computing environment," concluding that this somehow discloses the subject matter of independent claims 1, 10, and 12. However, contrary to assertions made in the Final Action, it remains readily apparent that Gupta fails to disclose or suggest *a component that compares an applied trust level* ***of an application*** *with a trust level of* ***a module called by the application*** *and regulates access of the application to* ***a distributed computing platform*** *based at least in part upon the comparison.*

In view of the foregoing, it is readily apparent that Gupta does not disclose or suggest the invention as recited in claims 1, 10, and 12 (and claims which depend therefrom). Accordingly, this rejection should be reversed.

B. Conclusion

For at least the above reasons, the claims currently under consideration are believed to be patentable over the cited references. Accordingly, it is respectfully requested that the rejections of claims 1-5 and 7-20 be reversed.

A credit card payment form is filed concurrently herewith in connection with all fees due regarding this document. In the event any additional fees may be due and/or are not covered by the credit card, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1063 [MSFTP150US].

Respectfully submitted,
AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24th Floor, National City Center
1900 East 9th Street
Telephone: (216) 696-8730
Facsimile: (216) 696-8731

VIII. Claims Appendix (37 C.F.R. §41.37(c)(1)(viii))

1. A system that regulates access to a distributed computing platform comprising:

a component that analyzes an application that requests access to the distributed computing platform, the component determines a level of access to the distributed computing platform and applies a trust level to the application corresponding to the determined level of access; and

a component that compares the applied trust level of the application with a trust level of a module called by the application and regulates access of the application to the distributed computing platform based at least in part upon the comparison.

2. The system of claim 1, the component that analyzes the application providing for inheritance of the trust level.

3. The system of claim 1, the component that analyzes the application providing for marking the application with at least one of states: (1) fully trusted, (2) run restricted, and (3) fail to load.

4. The system of claim 1, wherein the component that analyzes and the component that compares are stored in a Read Only Memory (ROM) in the platform.

5. The system of claim 1, wherein the component that analyzes and the component that compares are part of an operating system.

7. The system of claim 1, wherein the functionality of one or more Application Programming Interface (API) calls, when called by the application, are selectively restricted.

8. The system of claim 7, wherein selectively restricting the functionality of the one or more API calls includes restricting the functionality to read functions.

9. The system of claim 8, wherein selectively restricting the functionality of the one or more API calls includes terminating the application.

10. A system for regulating access to a distributed computing platform, comprising:

means for determining a trust level for an application, the application requesting access to the distributed computing platform;

means for applying the trust level to the application to regulate access to the distributed computing platform; and

means for regulating access of the application to the distributed computing platform by analyzing a trust level of a module called by the application.

11. The system of claim 10 further comprising means for applying the trust level to one or more modules called by the application.

12. A method for regulating access to a distributed computing platform, comprising the steps of:

determining a trust level for a first module called by an application, the application requesting access to the distributed computing platform; and

regulating access of the application to the distributed computing platform based at least in part upon the determined level of trust for the first module.

13. The method of claim 12 wherein determining the trust level for the first module further comprises the step of marking the first module with at least one of states: (1) fully trusted, (2) run restricted, and (3) fail to load.

14. The method of claim 12 wherein determining the trust level for the first module further comprises transmitting the first module to a verification program.

15. The method of claim 12 wherein regulating access to the distributed computing platform further comprises selectively aborting calls made to one or more APIs.

16. The method of claim 12 wherein regulating access to the distributed computing platform further comprises selectively terminating the first module.

17. The method of claim 12 wherein a program for determining the trust level for the first module is stored in a ROM in the platform.

18. The method of claim 12 wherein the logic for applying the trust level to regulate access to the platform is stored in a ROM in the platform.

19. The method of claim 12 wherein the trust level may be inherited.

20. The method of claim 12 wherein the trust level may be applied to one or more second modules called by the first module.

IX. Evidence Appendix (37 C.F.R. §41.37(c)(1)(ix))

None.

X. Related Proceedings Appendix (37 C.F.R. §41.37(c)(1)(x))

None.